

E-legitimationer enligt eIDAS

E-legitimationsnämndens analys av EU-förordningen om elektronisk identifiering och betrodda tjänster (EU nr 910/2014), regeringsuppdrag (N2015/2620/EF)

Dnr: 131 182017-15/9513 | 2015-12-16



**E-LEGITIMATIONS
NÄMNDEN**

Innehållsförteckning

1	Sammanfattning	2
2	Bakgrund och uppdrag	3
3	EU-förordningen i korthet	4
3.1	Utländska e-legitimationer obligatoriska från hösten 2018	4
3.2	Den svenska noden slussar trafik	5
3.3	Regler för att skapa tillit till utländska e-legitimationer	6
3.4	Kostnad för e-legitimeringar över landsgränserna	6
3.5	Förordning och genomförandeakter på EU-nivå	6
4	Begreppslista	7
5	Utländska e-legitimationer i svenska offentliga organs e-tjänster	8
5.1	De svenska offentliga organen har relativt goda förutsättningar	8
5.2	Ansvar för den svenska eIDAS-noden	9
5.3	Viktig möjlighet för digitaliseringen av offentlig sektor	10
5.4	E-tjänsterna hälsar välkommen	11
5.5	Möjlighet att koppla e-legitimationen till svenskt identitetsbegrepp	12
5.6	Nodens ansvar för behörighetsinformation bör vara begränsat	14
5.7	E-underskrifter helst på samma sätt som i Sverige	15
5.8	Myndigheter bör förnya sina riskanalyser	16
6	Privat sektors användning av utländska e-legitimationer	17
7	Svenskars möjligheter utomlands	18
7.1	Svenskars e-legitimering i utländska tjänster	18
7.2	Svenskars e-underskrifter som används utomlands	20
8	Tidplan och aktiviteter för genomförandet	21
9	Konsekvenser	22
9.1	Nyttor	22
9.2	Konsekvenser för offentliga organ till följd av obligatoriet	22
9.3	Konsekvenser för svensk e-legitimationsförsörjning	23
10	Sammanfattning av genomförda aktiviteter	23
11	Bilaga – Behov av utländska e-legitimeringar	24

1 Sammanfattning

Från den 29 september 2018 blir det enligt lag (Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, ”eIDAS”) obligatoriskt för svenska offentliga organ, och frivilligt i privat sektor, att i e-tjänster som erbjuder inloggning med e-legitimation erkänna utländska e-legitimationer som finns med i EU:s förteckning. Än så länge är det EU- och EES-länderna som ingår i eIDAS.

Det finns behov av att använda e-legitimationer över landsgränserna. Svenska myndigheter har som svar på en enkätfråga räknat upp en lång rad exempel inom bl.a. vård, omsorg, förskola och utbildning, beskattnings- och tullverksamhet, företagsregistrering, fastighets- och socialförsäkringsområdena. Den beslutade EU-förordningen ”eIDAS” innebär därför en viktig möjlighet till ytterligare digitalisering.

Införandet av e-legitimering över landsgränserna innebär inte enbart möjligheter utan även risker. Riskanalyser, säkerhetsrutiner, samt en samlad incidenthantering inom e-legitimationsområdet och att Sverige är aktivt internationellt, är exempel på viktiga åtgärder.

Regeringen har aviserat att E-legitimationsnämnden ska få utökat ansvar inom området och EU-förordningen specificerar att varje land ska tillhandahålla en s.k. nod för att underlätta interoperabiliteten mellan länderna. E-legitimationsnämnden föreslår att den svenska noden enligt eIDAS ska förmedla både offentlig och privat sektors trafik över landsgränserna inom området e-legitimationer och e-underskrifter.

E-legitimationslandet skickar med åtminstone namn, adress, födelsedag och ett personidentitetsbegrepp i varje e-legitimering. Personidentitetsbegreppet ska vara så beständigt som möjligt. Det finns inget gemensamt personidentitetsbegrepp inom eIDAS och vissa länder skickar olika personidentitetsbegrepp för olika områden.

Vissa svenska myndigheter ställer författningsstödda krav på att individen har ett svenskt personnummer eller fastställt samordningsnummer för att få behörighet att använda deras e-tjänst. Därför föreslår nämnden att Skatteverket ges i uppdrag att utreda möjligheten att, i vissa fall, bistå med koppling mellan den utländska e-legitimationen och individens svenska personnummer eller samordningsnummer.

Det är frivilligt för länderna att anmäla en eller flera e-legitimationer till EU:s förteckning. E-legitimationsnämnden bedömer att det finns behov för svenska medborgare och företag att få tillgång till e-legitimationer som kan användas utomlands.

Transaktionerna över landsgränserna görs utan ekonomisk ersättning vad gäller offentliga organs e-tjänster. Därför behöver frågan om ersättning till svenska e-legitimationsleverantörer regleras inom Sverige. Enligt förordningen finns det möjlighet för Sverige att skicka en pseudonym i personidentitetsbegreppet och denna möjlighet kan vara viktig att använda. Nämnden föreslår att regeringen utreder dessa frågor vidare. Nämnden bedömer att minst en svensk e-legitimation på den högsta tillitsnivån krävs för att tillvarata svenska intressenters möjligheter i utländska e-tjänster.

2 Bakgrund och uppdrag

En e-legitimation är en elektronisk identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg. E-legitimationen kan användas av enskilda och företrädare för företag eller myndigheter vid åtkomst till olika typer av e-tjänster. Den används också i andra sammanhang, som vid informationsutbyte mellan myndigheter och internt i organisationer.

Regeringens ambition är att e-legitimationer ska vara enkla och trygga för användare och villkoren för offentlig sektor att använda tjänsterna ska vara enkla, förutsägbara och kostnadseffektiva. På så sätt kan e-legitimationer stödja utveckling av e-förvaltning och även underlätta användning av e-tjänster i samhället.

Europaparlamentet och rådet har antagit förordning (EU) nr 910/2014 om e-legitimationer och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS). EU-kommissionen har under 2015 arbetat fram genomförandeakter på området.

Syftet med den nya EU-förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan privatpersoner, företag och offentliga myndigheter och därigenom öka effektiviteten hos offentliga och privata digitala tjänster samt i elektronisk affärsverksamhet och e-handel inom EU.

EU-förordningens regler är bindande och direkt tillämpliga. Regeringen har föreslagit riksdagen en lag med kompletterande bestämmelser till EU-förordningen. Termer och uttryck i lagen har samma betydelse som i EU-förordningen (se avsnitt 4). De nya bestämmelser som införs syftar till att komplettera EU-förordningens bestämmelser så att förordningen kan få fullt genomslag.

Regeringen skriver i sin lagrådsremiss att E-legitimationsnämnden föreslås få en utökad och tydligare roll när det gäller gränsöverskridande elektronisk identifiering genom att utreda och utveckla lösningar, tillhandahålla centrala tjänster, delta i pågående internationellt utvecklingsarbete samt ge stöd till myndigheter i frågor som rör

gränsöverskridande elektronisk identifiering. I budgetpropositionen för 2016 gör regeringen bedömningen att E-legitimationsnämndens verksamhet därför behöver stärkas genom en viss fortsatt anslagsfinansiering 2016–2019, se prop. 2015/16:1, utg.omr. 22, s. 120.

Eva Ekenberg, E-legitimationsnämndens kanslichef, är utsedd (dnr. N2015/480/EF) att företräda Sverige i eIDAS samarbetsnätverk (eng. ”Cooperation Network”, CN).

Regeringen lämnade i mars 2015 ett uppdrag (N2015/2620/EF) till E-legitimationsnämnden och Post- och telestyrelsen om att analysera EU-förordningen om elektronisk identifiering och betrodda tjänster. E-legitimationsnämndens uppdrag har varit att:

- analysera konsekvenser av de krav som ställs av eIDAS när det gäller personer som uppvisar en inom EU godkänd e-legitimation vid användning av svenska offentliga myndigheters elektroniska tjänster som kräver elektronisk identifiering, samt utreda och föreslå lösningar
- utreda och föreslå hur en lösning för gränsöverskridande elektronisk identifiering och underskrift kan utformas och erbjudas svenska intressenter i olika situationer (t.ex. privat, i tjänsten, för svenskar bosatta utomlands samt för företag, myndigheter och andra organisationer med gränsöverskridande verksamhet)
- bistå Näringsdepartementet i framtagandet av svenska ståndpunkter.

Denna rapport utgör E-legitimationsnämndens redovisning till regeringen.

3 EU-förordningen i korthet

3.1 Utländska e-legitimationer obligatoriska från hösten 2018

eIDAS¹ innebär ett obligatorium för offentliga organ att i sina nättjänster erkänna de e-legitimationer (system och medel för elektronisk identifiering) som är ömsesidigt erkända inom eIDAS, på motsvarande tillitsnivå eller högre, under förutsättning att nättjänsten använder elektronisk identifiering på åtminstone tillitsnivå ”väsentlig” enligt eIDAS. Motsvarande gäller frivilligt för privat sektor, samt frivilligt för offentliga organ och privat sektor i de nättjänster som accepterar elektronisk identifiering på tillitsnivå ”låg”.

Offentliga organ har en skyldighet att erkänna e-legitimationer senast ett år efter publicering i EU:s förteckning över ömsesidigt godkända e-legitimationer, vilket i sin tur

¹ [EU-förordningen om elektronisk identifiering, EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING \(EU\) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden](#)

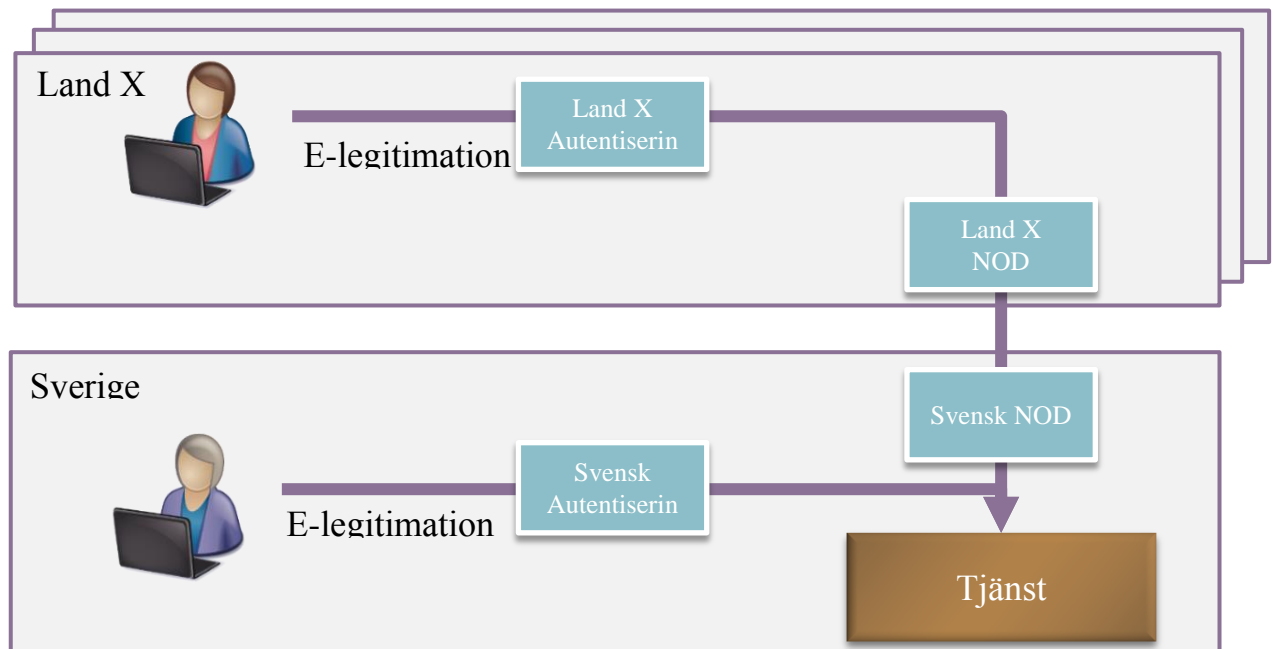
ska föregås av en sexmånadersperiod sedan information om e-legitimationen spreds av den anmälade medlemsstaten.

EU:s lista över erkända e-legitimationer öppnar den 29 september 2017 och det innebär att obligatoriet för offentliga organ i praktiken gäller från den 29 september 2018 under förutsättning att åtminstone en e-legitimation publiceras den första dagen och att information om e-legitimationen spreds minst ett halvår innan dess. Det är inte uteslutet att så kan bli fallet eftersom det redan nu finns länder som tidplansmässigt ligger i framkant, exempelvis Estland.

3.2 Den svenska noden slussar trafik

För att underlätta interoperabilitet över landsgränserna innehåller eIDAS en regel om att varje medlemsstat måste ha en nationell nod som ansvarar för att sköta trafiken som rör elektronisk identifiering till och från landet. Både aktuella svenska nättjänster (förlitande parter) i offentlig och privat sektor, och de av Sverige inom eIDAS anmälda e-legitimationsleverantörerna (identitetsleverantörer), ska således ta emot och skicka elektroniska identifieringar via den svenska eIDAS-noden.

Nodens roll när en individ i en svensk nättjänst använder en utländsk e-legitimation enligt eIDAS kan illustreras så här:



Figur 1: Illustration över nodens roll vid e-legitimeringar i svenska nättjänster

I den undre delen illustreras motsvarigheten inom Sverige, dvs. när en individ använder en svensk e-legitimation i samma nättjänst. Observera att medborgarskap saknar betydelse i sammanhanget, det är e-legitimationslandet som avgör innehållet.

3.3 Regler för att skapa tillit till utländska e-legitimationer

Tilliten till erkända e-legitimationer skapas genom att det anmälade landet går i god för e-legitimationen och är skyldigt att följa förordningens regler om bl.a. tillitsnivåer, anmälan, tillfälligt upphävande, återkallelse och skadestånd. På EU-nivå beslutade förfaranden med sakkunnighetsbedömning, ett samarbetsnätverk mellan medlemsstaterna, erfarenhetsutbyte, omvärldsbevakning, kontaktpunkter i varje medlemsstat, samt gransknings- och incidenthanteringsrutiner, ska också borga för tillit.

3.4 Kostnad för e-legitimeringar över landsgränserna

Det är kostnadsfritt för svenska myndigheter i förhållande till utlandet att ta emot erkända e-legitimationer över landsgränsen. Det är även kostnadsfritt för de andra medlemsstaternas offentliga organ att ta emot svenska e-legitimationer. Däremot kan ersättningar regleras inom respektive land. EU-förordningen säger inget om prisnivån för privat sektor att ta emot utländska e-legitimationer i sina nättjänster, men förordningen anger att det är den medlemsstat som anmäler en e-legitimation till EU:s lista som sätter priset.

3.5 Förordning och genomförandeakter på EU-nivå

EU-förordningen ”eIDAS” ([Europaparlamentets och rådets förordning \(EU\) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden](#)) är publicerad på nätet och finns översatt till svenska.

Inom området elektronisk identifiering finns det utöver EU-förordningen fyra beslutade genomförandeakter (med beslutsnummer/länk och förordningens artikel inom parentes):

1. samverkan rörande elektronisk identifiering ([2015/296](#), art. 12.7)
2. tillitsramverk (tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering, [2015/1502](#), art. 8.3)
3. interoperabilitetsramverk ([2015/1501](#), art. 12.8)
4. förutsättningar, format och förfaranden för anmälan ([2015/1984](#), art. 9.5)

Genomförandeakterna finns översatta till svenska. Dessutom har EU-kommissionen tagit fram en teknisk specifikation som konkretiserar genomförandeakten om interoperabilitet, utkast till incidenthanteringsrutin, samt en vägledning för tillitsramverket. Ett särskilt krav avseende interoperabilitet är rätten för medlemsstaterna till s.k. middleware. Denna rätt innebär en skyldighet för alla de andra medlemsstaterna att i sina noder inkludera en

för den första medlemsstaten specifik programvara. Detta är aktuellt för e-legitimering från vissa länder (i dagsläget Österrike och Tyskland) och är en följd av att lagen i dessa länder inte tillåter centrala noder för gränsöverskridande legitimering.

4 Begreppslista

EU-förordningen (artikel 3) använder sig av bl.a. följande definitioner:

Begrepp	EU-förordningens definition
Elektronisk identifiering	En process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.
Medel för elektronisk identifiering	En materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.
Personidentifieringsuppgifter	En uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.
System för elektronisk identifiering	Ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.
Autentisering	En elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.
Förlitande part	En fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster.
Offentligt organ	En statlig, regional eller lokal myndighet, ett organ som lyder under offentlig rätt eller en sammanslutning som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentlighetsorgan, eller en privat enhet som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.
Elektronisk underskrift	Uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.
Avancerad elektronisk underskrift	En elektronisk underskrift som uppfyller kraven enligt artikel 26.
Kvalificerad elektronisk underskrift	En avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

5 Utländska e-legitimationer i svenska offentliga organs e-tjänster

Införandet av eIDAS innebär stora möjligheter för svenska offentliga myndigheter att förbättra åtkomsten till digital service. För dem med utländska e-legitimationer kan ärenden därmed bli enklare och säkrare att hantera digitalt, jämfört med att skicka papper eller personliga besök.

5.1 De svenska offentliga organen har relativt goda förutsättningar

Nämndens bedömning:

eIDAS bidrar med viktiga tillitsskapande regler och tekniska specifikationer för elektronisk identifiering som tidigare saknats vid användning av e-tjänster över landsgränserna.

Förutsättningarna för det obligatoriska införandet av eIDAS är goda för de offentliga myndigheter som finns med i den nationella identitetsfederationen och ganska goda för de organisationer som av annat skäl i sina e-tjänster redan använder standarden [SAML 2](#).

Regeringen har med hjälp av bl.a. E-legitimationsnämnden och andra svenska myndigheter varit aktiv i EU:s arbete med att specificera tillitsnivåer och interoperabilitet på EU-nivå. E-legitimationsnämnden har haft de nya EU-reglerna i åtanke kraven på svenska e-legitimationer har tagits fram ([Svensk e-legitimation](#)). De nya svenska tillitsnivåerna 3 och 4 liknar² därför eIDAS tillitsnivåer ”väsentlig” och ”hög”.

Den internationella e-legitimationstrafiken enligt eIDAS följer samma väletablerade standard (SAML 2) som många e-tjänster redan använder vid inloggning med e-legitimation (t.ex. kommuner, landsting och några statliga myndigheter). SAML 2 förekommer även inom behörighetsfederationer, exempelvis inom vård- och omsorg (Sambi) och universitetsvärlden (SWAMID). Den nationella offentliga identitetsfederationen (Svensk e-legitimation) använder också den standarden.

Även om en e-tjänst skulle ligga på något annat upphandlingsavtal än Svensk e-legitimation för sina e-legitimeringar men ändå använder SAML 2, kan införandet gå relativt smidigt under förutsättning att man som offentligt organ lämnar uppgifter (metadata) om sina e-tjänster till den kommande svenska noden och följer de tekniska specifikationerna från den svenska nodansvariga myndigheten.

² Tillitsnivåerna skiljer sig f.n. en aning på den högsta tillitsnivån. Eftersom det inte är tillåtet med s.k. degradering, där noden gör om en e-legitimering på tillitsnivå ”high” till tillitsnivå 3 som om den var en e-legitimering tillitsnivå 3, måste antingen de svenska tillitsnivåerna justeras i enlighet med eIDAS eller någon annan lösning arbetas fram.

De tekniska förutsättningarna är i och med Svensk e-legitimations tekniska ramverk i stora drag harmoniserade gentemot eIDAS motsvarighet. Sverige har även deltagit i EU:s pilotprojekt på området (STORK, STORK 2 och E-sens) och det finns därmed kompetens med praktisk erfarenhet att tillgå. Allt detta sammantaget underlättar det svenska införandet.

5.2 Ansvar för den svenska eIDAS-noden

Nämndens förslag:

Nämnden föreslår regeringen att Sveriges nod enligt eIDAS blir E-legitimationsnämndens ansvar.

Noden bör hantera såväl inkommande som utgående elektroniska identifieringar till och från Sverige, samt transaktioner för e-underskrifter. Noden bör förmedla både offentlig och privat sektors trafik över landsgränserna inom området e-legitimationer och e-underskrifter.

Tidplanen bör vara att noden ska kunna ta emot e-legitimeringar från utlandet i produktionsmiljö så snart det är möjligt, men att nodens kapacitet från början kan vara begränsad för att senare, över tid, kunna skalas upp successivt.

Noden föreslås bli anslagsfinansierad, åtminstone med avseende på svenska offentliga organs erkännande av utländska e-legitimationer vars åtagande är en direkt följd av EU-förordningen. I finansieringen behöver ingå medel som täcker den svenska noden, incidentrapporteringsrutiner, samordning, information till svenska offentliga myndigheter och andra svenska målgrupper, samt täcker övriga uppdrag som regeringen vill delegera, exempelvis den svenska kontaktpunkten och vissa svenska roller i EU-samarbetet.

E-legitimationsnämnden föreslås få rätt att ange rutiner för den svenska noden, inte minst rörande tekniska krav.

Skälen för förslaget:

eIDAS stipulerar att varje medlemsstat ska ha en s.k. nod som ska sköta e-legitimationstrafiken till och från landet. Noden har krav på sig att inte lagra personuppgifter, bortsett från undantaget i förordningens artikel 9.3.

Det framgår av den tekniska specifikationen för interoperabilitet att noden kan vara uppbyggd på olika sätt, vilket innebär att det kan finnas utbyggnadsmöjligheter över tid. I början är det sannolikt enklast i kontakter med andra länder, och inom landet, om Sverige har endast en landsnod och att det är ett myndighetsansvar. eIDAS stipulerar att privat sektor (som förlitande part) ingår frivilligt. Därför behöver landsnoden även slussa

trafiken för privat sektors räkning, även om införandet av offentlig sektors trafik behöver ges högre prioritet med anledning av obligatoriet. Att börja med endast en landsnod underlättar hantering av metadata och kan på sikt kanske underlätta för s.k. attributtjänster.

Noden måste utformas på ett säkert sätt och på ett sätt som värnar om den personliga integriteten. Noden kommer på sikt eventuellt att klassas som kritisk infrastruktur och detta behöver beaktas vid utveckling och utformning av noden redan inledningsvis. Vid en eventuell upphandling av utveckling- och driftleverantör behöver riskanalys och bedömning göras med avseende på om upphandlingen ska göras inom ramen för en säkerhetsskyddad upphandling.

I noden får Sverige inte lagra personuppgifter från utländska identitetsintyg. Eventuella behov av registerföring av personuppgifter inom ramen för den ansvariga myndighetens verksamhet har inte framkommit. Däremot måste den nodansvariga myndigheten ges rätt att konvertera mellan olika tekniska format och den behöver få möjlighet att komplettera den svenska översättningen av identitetsintyget med personuppgifter som är tillgängliga via t.ex. Navet och motsvarande. Nodansvarig myndighet behöver kunna stipulera interoperabilitet inom Sverige och realisera noden som en aktör i den svenska identitetsfederationen. Dessutom måste s.k. middleware-programvara från vissa andra medlemsstater hanteras av den svenska noden.

Att ge en myndighet ansvaret för den svenska noden måste inte hindra att andra verksamheter kan bedriva testverksamhet inom området. Initialt kan några olika arkitekturmönster för noden behöva testas praktiskt för att finna den mest effektiva lösningen.

5.3 Viktig möjlighet för digitaliseringen av offentlig sektor

Nämndens bedömning:

Svenska offentliga myndigheter har behov av att ta emot utländska e-legitimationer.

En vanligt förekommande fråga är i vilka svenska offentliga digitala tjänster det finns direkta behov av att ta emot utländska e-legitimationer.

E-delegationen konstaterade i sitt slutbetänkande En förvaltning som håller ihop (SOU 2015:66, s. 33) att det finns behov av att utländska medborgare ska kunna legitimera sig med en utländsk e-legitimation i svenska e-tjänster.

E-legitimationsnämnden tog upp frågan i E-legitimationsenkäten (september 2015). Svaren visade att 71 % av kommunerna (82 av de 115 som besvarat frågan av totalt 165

respondenter), landstingen och 61 % av de statliga myndigheterna (35 av de 57 som besvarat frågan av totalt 140 respondenter) ser att de är berörda av eIDAS-införandet.

Behoven finns exempelvis inom:

- starta företag och söka tillstånd
- vård och omsorg
- förskola och skola
- sjukpenning
- beskattning, rut-/rotavdrag
- tullverksamhet
- Mina meddelanden (minameddelanden.se).

Idag hanteras sådana ärenden många gånger via osäkra eller krångliga identifieringsförfaranden, osäkra papperskanaler eller via kostnadskrävande onödiga personliga besök. Se bilaga 1 för fler exempel.

5.4 E-tjänsterna hälsar välkommen

Nämndens bedömning:

Varje offentligt organ behöver bedöma om en individ ska släppas in i en tjänst, eller inte. Detta gäller oavsett vilken e-legitimation som visas upp.

Myndigheten måste själv meddela att e-legitimationen är erkänd men att användaren tyvärr inte kan göra något i e-tjänsten om det är så att individen saknar behörighet till e-tjänsten. Ett sådant exempel är om e-tjänsten kräver en viss uppgift från e-legitimationen och den uppgiften saknas.

I skrivande stund krävs i praktiken svenskt personnummer för att kunna använda svenska offentliga e-tjänster som kräver e-legitimation.

Användaren kanske ännu inte har något personidentitetsbegrepp som den svenska myndigheten accepterar. eIDAS innebär inte något obligatorium beträffande behörighetsregler utan endast att e-tjänsten har erkänt den utländska, inom eIDAS godkända, e-legitimationen.

I några verksamheter kommer den utländska e-legitimationen att räcka och det är då en fördel om det utländska personidentitetsbegreppet används i första hand. Ett sådant exempel är när en företagare skriver under en handling hos Bolagsverket. Underskriften är rättshandlingen. Det kanske i vissa andra fall kan räcka om individen i e-tjänsten anger relevanta uppgifter manuellt. Frågor om språk behöver ses över, enligt svensk lag behöver exempelvis vissa handlingar vara på svenska.

När behörighet saknas måste användaren kunna få ett meddelande om att e-legitimationen visserligen är erkänd men att det tyvärr inte går att göra något i tjänsten. Samma sak gäller när behörighet av andra skäl saknas. Förfarandet kan även vara bra som en säkerhetsmetod när det står stora värden på spel och införandet av eIDAS ännu är i sin linda. För att uppnå syftet med eIDAS-förordningen behöver däremot ett antal myndighetsärenden kunna kopplas till individens svenska personidentitetsbegrepp.

5.5 Möjlighet att koppla e-legitimationen till svenskt identitetsbegrepp

Nämndens förslag:

Att regeringen ger Skatteverket i uppdrag att utreda förutsättningarna för att använda utländska e-legitimationer inom svenska digitala myndighetstjänster där det finns behov av en koppling mellan den utländska e-legitimationen och det svenska personnummer eller samordningsnummer som individen redan har eller har tilldelats av annan anledning. Utredningen ska även lämna de författningsförslag som bedöms lämpliga.

Skälen för förslaget:

Svenska myndigheter har författningsstödda krav på att få tillgång till kvalitetssäkrade personuppgifter för att kunna utföra sina uppdrag väl, och behöver i ett flertal e-tjänster vara säkra på användarens identitet. Det andra landet går i god för individens identitet och den utländska e-legitimationstjänsten lämnar ifrån sig ett fåtal personuppgifter i samband med individens e-legitimering. Som ett minimum skickas namn, nuvarande adress, födelsedag och personidentitetsbegrepp ("minimum data set").

För en del e-tjänster räcker dessa personuppgifter. E-legitimationslandet åtar sig att e-legitimationslandets personidentitetsbegrepp i e-legitimeringen ska vara så "beständigt som möjligt". Vissa e-legitimationsländer med användare som har stort behov av svenska e-tjänster kommer att skicka personidentiteter vars beständighet motsvarar svenska personnummers. För att undvika missförstånd kan det vara värt att betona att inget nytt personidentitetsbegrepp på EU-nivå är på väg att införas.

Huvudfrågan är om detta kan förenas på ett sätt som både leder till en säker och god digital service, effektiv myndighetsverksamhet och samtidigt värnar om den personliga integriteten. Vissa e-tjänster har författningsstödda behov av att kunna koppla e-legitimeringen till ett svenskt samordningsnummer eller personnummer för att användaren ska få använda e-tjänsten. Ett behov är därför att individer, på ett frivilligt och säkert sätt, kan koppla sin EU-godkända utländska e-legitimation till sitt redan

utfärdade svenska personnummer eller identitetsstyrkta samordningsnummer, alternativt kunna få visa upp sin e-legitimation i samband med att personnumret eller samordningsnumret utfärdas.

E-delegationen tar upp detta behov i sitt slutbetänkande En e-förvaltning som håller ihop (SOU 2015:66):

”Svenska myndigheter kan i dag rekvirera samordningsnummer från Skatteverket för personer som saknar svenskt personnummer om det behövs vid viss ärendehantering. Förutsättningarna för en sådan rekvisition är emellertid begränsade, bland annat ska individens identitet vara styrkt. Skatteverket lagrar uppgift om bland annat födelsetid, namn och adress i Sverige, men saknar författningsstöd för att lagra personens identitet från hemlandet. Ett sådant författningsstöd finns endast för personnummer som personen har tilldelats i annat nordiskt land. För att hantera detta med minsta möjliga ändring av svenska e-tjänster behöver den ansvariga myndigheten, Skatteverket, ges författningsstöd att dels få tilldela dessa personer samordningsnummer eller liknande identifikationsbegrepp, dels få lagra kopplingen till den utländska e-legitimationen. Identifiering av utländska personer behöver möjliggöras.”

Ett visst arbete kring detta gjordes i samband med den första EU-piloten (STORK), men det behövs mer för att täcka behoven, som kan delas in i några olika fall.

Ett fall är om personen i fråga redan har ett identitetsstyrkt svenskt samordningsnummer eller personnummer som behöver kopplas ihop med personens utländska e-legitimation. Detta måste ske på ett tillräckligt säkert sätt. Ett annat fall är om den utländska e-legitimationen, på tillräcklig tillitsnivå, delvis ligger till grund för den säkra identifiering som den svenska myndighet som rekvirerar samordningsnumret är skyldig att göra.

Inom en rad offentliga verksamheter, t.ex. fastighetsägande, företagande och beskattning, finns författningsstöd för att hantera den svenska personidentiteten. Då har individen i fråga normalt sett en varaktig relation med svenska myndigheter och måste både inneha och kunna visa upp ett personnummer eller ett identitetsstyrkt samordningsnummer. Ett syfte med detta är att värna om kvalitet och effektivitet i verksamheten. EU-förordningen som helhet är, jämfört med dagens pappershantering, särskilt intressant för den exekutiva myndighetsverksamheten där det andra landet har en skyldighet att bistå med spårbarhet som kan användas vid handräckning.

Skatteverkets utredning innebär inte någon generell möjlighet för den som saknar ett svenskt identifikationsbegrepp att på egen begäran tilldelas ett sådant nummer. Med hänsyn till tidsutrymmet för att implementera en lösning är relativt kort, faller det sig naturligt att börja med offentlig sektor innan lösningen anpassas för privat sektor. Genom

att noden införs så finns lösningar som möjliggör att privat sektor skulle kunna använda utländska e-legitimationer, dock utan någon automatisk myndighetskoppling till svenskt person- eller samordningsnummer.

På lång sikt, vid en eventuell markant ökning av antalet myndighetsärenden och antalet nya samordningsnummer, finns det risk för att samordningsnumren inte räcker till. Frågan om ett nytt svenskt, nationellt personidentitetsbegrepp för utländska personer kan komma att behöva utredas i särskild ordning, i takt med att trafiken över landsgränserna ökar.

5.6 Nodens ansvar för behörighetsinformation bör vara begränsat

Nämndens bedömning:

Arbetet kring behörighetsinformation bör i första hand bedrivas sektorvis. Den svenska nodens ansvar för behörighetsinformation bör vara begränsat till att förmedla ett fåtal uppgifter från start.

eIDAS innehåller inga regler om behörighetsinformation (behörighetsattribut), t.ex. sektorspecifika personidentitetsbegrepp, men hindrar inte heller noderna från att förmedla behörighetsinformation. EU-piloten STORK 2 var inriktat på att bredda omfattningen från elektronisk identifiering över landgränserna till att även omfatta utbyte av behörighetsinformation. Pilotarbetet har stött på många hinder.

Varje e-tjänst ställer normalt sett krav på användarens behörighet för användning av e-tjänsten. Användaren kan behöva vara i en viss livshändelse, eller ha viss ålder, familjeband, körkort, lärarlegitimation, läkarlegitimation etc. för att kunna ges behörighet att använda en viss e-tjänst eller dess funktioner.

Behörighetsinformation kan inhämtas på olika sätt. För det första kan vissa uppgifter kanske hämtas maskinellt från det andra landet givet författningsstöd eller medgivanden från individen, för det andra kan individen mata in uppgifter i e-tjänsten och för det tredje kan underlag ha kommit in i förväg.

Ytterligare ett tillvägagångssätt kan vara att begära in en handling från individen som med hjälp av s.k. betrodda tjänster har säkrats vara utgiven från rätt part. Detta kan för Sveriges del vara ineffektivt eftersom nättjänsterna kan vara bättre betjänta av välstrukturerade elektroniska uppgifter.

För att nå EU:s och regeringens mål för digitalisering behöver Sverige samverka om behörighetsinformation med Danmark, Norge och Finland och andra länder Sverige har

stort utbyte med. Samarbetet kan ske sektorvis, på motsvarande sätt som samverkan redan bedrivs inom exempelvis vården, tullverksamhet och utbildningsområdet.

Som en vidareutveckling, inom t.ex. Norden eller som ett tillägg till eIDAS på EU-nivå, skulle man kunna tänka sig att länderna kunde komma överens om att följa principerna enligt genomförandeakten för interoperabilitet, samt standarden enligt ”Technical Specifications”, även för behörighetsinformation (attribut). Det betyder i så fall att SAML 2 skulle vara förstahandsvalet och att det över tid därmed utvecklas metadata för behörighetstjänster. Grundprinciper för auktorisation skulle kunna slås fast i en svensk vägledning, eller i ett blivande ramverk för Norden, alternativt på EU-nivå om det vore möjligt.

5.7 E-underskrifter helst på samma sätt som i Sverige

Nämndens bedömning:

E-underskrifter i svenska myndigheters e-tjänster bör i första hand utföras på samma sätt som de är planerade att utföras inom den svenska offentliga identitetsfederationen, dvs. utföras med stöd av ett identitetsintyg för underskrift kompletterat med myndighetens underskriftstjänst. Ett tillägg till den svenska noden kan behöva hantera den användardialog och funktionalitet som den utländska e-legitimationen saknar.

Redan underskrivna dokument som kommer till Sverige behöver valideras i Sverige. E-legitimationsnämnden skulle kunna ges i uppdrag att tillhandahålla en sådan valideringstjänst.

Eventuella andra e-underskriftsvarianter behöver utredas i särskild ordning.

Av förordningen följer att den svenska noden ansvarar för att förmedla även identitetsintyg för underskrift, med tillhörande förfrågan.

Av EU-förordningen följer att en avancerad elektronisk underskrift ska uppfylla följande krav:

- den ska vara unikt knuten till undertecknaren,
- undertecknaren ska kunna identifieras genom den,
- den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll, och
- den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas

Givet att myndigheten har rätt att ange för användaren hur en underskrift ska göras och den utländska e-legitimationsleverantören kan hantera identitetsintyg för underskrift

bedömer E-legitimationsnämnden att det är möjligt att hantera e-underskrifterna i eIDAS-fallet på exakt samma sätt som e-underskrifterna enligt Svensk e-legitimation. Det innebär att e-tjänsten begär en ny legitimering (för underskrift) och tillsammans med sedvanlig rutin åstadkommer en underskrift.

Nationella regler om form går före eIDAS-regler om form, men det kanske kan finnas fall, t.ex. med redan underskrivna e-dokument, då kvalificerade e-underskrifter behöver användas. Läs mer i PTS rapport till regeringen om betrodda tjänster (samma regeringsuppdrag).

Det kan finnas ett effektiviseringsvärde om en statlig myndighet ges i uppdrag att sköta validering av underskrifter för andra statliga myndigheters räkning där så är lämpligt. Utredning av detta behöver göras i särskild ordning.

Utredning av ytterligare e-underskriftsfrågor kan komma att behöva göras i samband med införandet av eIDAS, i takt med att användningsmönstren klarnar.

5.8 Myndigheter bör förnya sina riskanalyser

Nämndens bedömning:

Införandet av e-legitimering över landsgränserna innebär inte enbart möjligheter utan även risker för svenska myndigheter. Riskerna behöver hanteras dels genom myndigheternas kvalitetssäkrar sitt val av tillitsnivå per e-tjänst, dels med hjälp av säkerhetsrutiner. Dessutom behöver Sverige ha en väl fungerande samlad incidenthantering inom e-legitimationsområdet och vara aktivt inom eIDAS samarbetsnätverk (CN).

Dagens bristande pappersrutiner och bristande elektroniska lösningar över landsgränserna ersätts av morgondagens e-legitimeringar. eIDAS innebär en möjlighet till bättre ordning, effektivisering och god service, men innebär även risker för ökat genomslag för cyberbrottsligheten och andra säkerhetsrisker. Riskerna ökar i takt med att antalet godkända e-legitimationer, och därmed antal möjliga angreppspunkter, ökar. När myndigheterna fram till nu har övervägt vilka e-tjänster som ska kräva en svensk e-legitimation har man kanske inte övervägt krav på tillitsnivå i förhållande till den kommande internationella e-legitimationstrafiken. Myndigheter får samtidigt inte diskriminera godkända utländska e-legitimationer gentemot de svenska e-legitimationerna och tillitsnivåerna behöver därför harmoniseras mellan Sverige och eIDAS, vilket bedöms beröra den högsta tillitsnivån.

Därför behöver svenska myndigheter överväga e-tjänstens krav tillitsnivå ännu en gång. E-legitimationsnämnden arbetar för närvarande fram en vägledning för e-tjänsteägare som kan vara till hjälp vid denna bedömning.

Myndigheterna kan även behöva se över att det finns fungerande loggar och andra säkerhetsrutiner så att det blir möjligt att backa tillbaka transaktioner om ett land brister i sin e-legitimationskvalitet. Inom vissa verksamheter kan myndigheten behöva överväga möjligheter att stänga av trafik. Analys mot Lissabonfördraget och undantag enligt eIDAS är i sammanhanget att se som möjligheter.

Incidenthanteringen måste följa regler enligt eIDAS och Myndigheten för samhällsskydd och -beredskap. Detta kommer sannolikt att bli ett omfattande arbete.

Spårbarheten är en förutsättning för att uppnå rättsverkan, dvs. spårbarhet måste finnas i hela kedjan av aktörer för att kunna påvisa oavvislighet och där varje aktör måste kunna bistå vid behov. Myndigheten som är ansvarig för noden bör få ett uttalat ansvar för att bistå svenska tjänster när utökad spårbarhet krävs. Frågor från andra länder kanaliseras via den svenska nodansvariga myndigheten.

Hindren mot att snabbt och på bred front införa utländska e-legitimationer i svenska myndigheters e-tjänster kan i vissa sammanhang ses som en fördel. Om det exempelvis rör sig om utbetalning av belopp, beviljande av vapenlicens eller samhällskritiska system, kan det vara bra att det finns inbyggda trögheter, t.ex. om det finns svårigheter för svenska myndigheter att få tillgång till betrodda elektroniska behörighetsuppgifter från utlandet.

Ett möjligt tillvägagångssätt är att vidareutveckla e-tjänsterna i en klok ordning, så att de e-tjänster som både har a) stora behov och b) lägre risk än alternativet, anpassas först.

6 Privat sektors användning av utländska e-legitimationer

Nämndens bedömning:

Den svenska eIDAS-noden bör förmedla även privat sektors e-legitimationstrafik enligt eIDAS. Privat sektor deltar på frivillig grund.

Självkostnadsfinansiering av den svenska eIDAS-noden kan vid behov övervägas.

Elektronisk identifiering och elektronisk underskrift är viktiga förutsättningar för att medborgare ska kunna använda digitala tjänster i samhället i stort. Privat sektors digitala tjänster omfattas frivilligt i eIDAS-förordningen. För att underlätta andra länders eIDAS-trafik till och från Sverige bör staten ta på sig ett förmedlingsansvar fram tills det är

lämpligt att eventuella noder inom enskild sektor tar över ansvaret. Detta förfarande innebär att E-legitimationsnämnden, lämpligen reglerat genom avtal, kommer att hålla viss information (metadata) om nättjänster utanför den offentliga federationen.

Om förmedling av privat sektors trafik skulle bli kostnadsdrivande för staten kan det komma att bli aktuellt med självkostnadsfinansiering. Frågan kan hanteras av staten i takt med att trafikflöden eller kravbilden innebär särkostnader av betydelse.

Den internationella prislistan för enskild sektors utländska e-legitimeringar är i skrivande stund oklar.

7 Svenskars möjligheter utomlands

7.1 Svenskars e-legitimering i utländska tjänster

Nämndens förslag:

Nämnden föreslår regeringen utreder vidare förutsättningarna för svenska intressenters möjligheter utomlands. Utredningsfrågorna (utöver Sveriges vilja som medlemsstat) gäller bl.a. ersättning till svenska e-legitimationsleverantörer, skadestandsreglering och andra eventuella villkor, val av delegering av ansvaret att affärsförhandla med e-legitimationsleverantörer för statens räkning, val av vilken part som anmäla e-legitimationer ("eID systems and means") till kommissionen, samt om pseudonym för personnummer ska användas.

Nämndens bedömning:

Regeringen, E-legitimationsnämnden och id-kortsupphandlande offentliga myndigheter bör verka för svenska intressenters möjlighet till svenska e-legitimationer som kan användas utomlands enligt eIDAS.

Nämnden bedömer att åtminstone en e-legitimation på tillitsnivå hög behöver erbjudas svenska medborgare att använda utomlands enligt eIDAS.

Skälen för förslaget:

I takt med att utländska tjänster digitaliseras, inte minst inom offentlig verksamhet, är det viktigt för svenska individer (privatpersoner och representanter för företag och andra organisationer) att kunna identifiera sig elektroniskt i utländska tjänster. Därför behöver Sverige dra nytta av de möjligheter eIDAS erbjuder. I samtalen med företrädare för andra länder har det framkommit att vissa utländska e-tjänster kommer att kräva den högsta tillitsnivån.

Givet den rådande svenska prismodellen för e-legitimeringar behöver svenska eID-leverantörer få ersättning för svenskars användning av e-legitimationen i utländska e-tjänster. Ett möjligt upplägg vid små volymer kanske skulle kunna vara att den utländska myndighetstrafiken gentemot svenska eID-leverantörer räknas som en upphandlande myndighet, och att E-legitimationsnämnden ikläder sig det ansvaret.

Det står eID-utfärdare fritt att erbjuda sina målgrupper e-legitimationer och om det finns avtal med den svenska staten om eIDAS, kan e-legitimationen användas utomlands av målgrupperna i enlighet med eIDAS. Offentliga organisationer bör exempelvis överväga individers möjligheter till e-legitimationer som får användas till eIDAS kopplat till de id-kort som upphandlas för privatpersoners, offentliganställdas och uppdragstagares räkning. Privata företag har möjlighet att göra samma sak när de upphandlar id-kort eller e-legitimationer för sina anställda och uppdragstagare.

Det är angeläget att inkludera organisationers behov av elektronisk identifiering av system (betrodd tjänst), samt följa den fortsatta utvecklingen inom eIDAS beträffande juridiska personer. Det är viktigt att det finns en uttalad minimirekommendation som alla tillhandahållare av betrodda tjänster är skyldiga att följa gällande krav på krypto- och hashalgoritmer, samt nyckellängder. I PTS slutrapport ”Redovisning av regeringsuppdrag avseende konsekvenser av eIDAS-förordningen gällande betrodda tjänster ” beskrivs behovet av genomförandeakt på kryptoområdet. Behovet gäller även området elektronisk identifiering.

Den svenska eID-marknaden kan inte sägas vara särskilt välfungerande. E-legitimationsnämndens upphandling av svenska e-legitimationer på tillitsnivå väsentlig varit utlyst i snart två år utan att någon privat eID-utfärdare eller eID-leverantör ansökt. Därför kan det bli nödvändigt att staten eller en annan offentlig aktör vidtar ytterligare åtgärder för att svenskar ska ha tillräckliga e-legitimationsmöjligheter utomlands.

Det svenska personnumret används mycket ofta och finns genom den svenska offentlighetsprincipen relativt tillgängligt via internet. För att värna om svenskars personliga integritet kan det därför kanske vara viktigt för svenskarna att Sverige använder möjligheten till pseudonym vid användning av en svensk e-legitimation utomlands.

Om ett nytt personidentitetsbegrepp skulle bli aktuellt att införa som pseudonym, finns det vissa önskvärda egenskaper att tänka på. Pseudonym-begreppet bör utformas så att det

- inte är värdebärande, t.ex. inte beskriva födelsedag
- är unikt

- är kort och enkelt att förstå
- är stabilt över tid
- är möjligt att verifiera med kontrollsiffra
- inte krockar med annan nummerserie av betydelse
- är uppbyggt så att det kan innehålla både bokstäver och siffror
- ska kunna lösas med hjälp av en slumpvalsgenerator

Det är viktigt för den enskilde att känna till sin eventuella pseudonym och spårbarheten behöver säkras.

7.2 Svenskars e-underskrifter som används utomlands

Nämndens bedömning:

Frågan om svenska intressenters underskriftsmöjlighet i utländska e-tjänster behöver följas. I första hand vore det bra om utländska e-tjänster gör som det är planerat att svenska offentliga e-tjänster ska göra och i andra hand bör lösningar som tillhandahålls av marknaden användas. Den svenska staten kan behöva vidta ytterligare åtgärder om det visar sig att dessa alternativ inte räcker till.

Man kan tänka sig att utländska e-tjänster följer den kommande svenska rutinen för e-underskrifter och i så fall behöver inget särskilt göras från svenskt håll. Men man kan även tänka sig andra rutiner i utlandet. En fråga att överväga är om en svensk myndighet behöver bidra med svenskt nationellt stöd för avancerade e-underskrifter i vissa utländska fall.

Det finns för närvarande en mycket begränsad eller ingen nationell efterfrågan på kvalificerade elektroniska underskrifter. Det finns däremot ett behov av sådana tjänster för gränsöverskridande användning. Det är därför viktigt att det finns tillhandahållare av kvalificerade betrodda tjänster på den svenska marknaden så att svenska företag kan köpa tjänster för att, t.ex. kunna lämna anbud i offentlig upphandling och skriva under elektroniska fakturor i de medlemsländer där det ställs formkrav på att kvalificerade betrodda tjänster används för sådana förfaranden. Om sådana leverantörer saknas om några år kan den svenska staten komma att behöva vidta ytterligare åtgärder.

Läs mer om betrodda tjänster i Post- och telestyrelsens slutrapport från detta regeringsuppdrag.

8 Tidplan och aktiviteter för genomförandet

Obligatoriet för offentliga myndigheter i september 2018 medför att konkreta aktiviteter behöver genomföras under 2016. Specifikation och tester av svensk nodfunktionalitet måste genomföras under det närmaste året. I närtid behövs information till alla svenska myndigheter och ramavtalsleverantörer. Statliga myndigheter under regeringen kan behöva få i uppdrag av regeringen att kartlägga sina e-tjänsters anslutning till eIDAS.

Sverige behöver agera som kontaktpunkt och i samarbetsnätverket på EU-nivå. Inom E-sens förs fortsatt dialog med t.ex. Norge och Danmark, som sedan behöver gå över i frivilliga initiativ enligt eIDAS.

En offentlig utredning om svenskers möjligheter utomlands behöver startas så snart som möjligt. Lagförslag om att på frivilliga grund få registrera e-legitimationer i folkbokföringen behöver tas fram och beslutas. En rättslig analys kring personuppgiftsansvaret kopplat till noden behöver genomföras. En första arkitektur för noden behöver beskrivas och beslutas, samt realiseras.

En första version av den svenska noden att produktions sättas och de första frivilliga svenska e-tjänsterna kan därmed gå i produktion enligt reglerna för frivilliga initiativ enligt eIDAS-förordningen. De offentliga initiativen bör med hänsyn till obligatoriet prioriteras högre än privat sektors initiativ, om resurskonflikt inom offentlig sektor skulle uppstå. De möjliga frivilliga initiativ enligt eIDAS som har framkommit under denna utredning är dels Verksamt.se (företagsregistrering och torgtillstånd), dels Vara/Liiv (läkemedelsregistrering, en första pilot inom vårdsektorn).

Att via en utländsk e-legitimering få tillgång till svenskt personnummer eller samordningsnummer måste komma på plats för att nå framgång i ett antal e-tjänster, om än att det inte är nödvändigt i alla tänkbara e-tjänster.

Stöd till myndigheters breddinförande behövs för att uppnå nytta. Från 2018-09-29 är utländska erkända e-legitimationer obligatoriska i offentliga e-tjänster.

Därefter genomförs fortsatt vidareutveckling av noden och inkoppling av fler e-tjänster så att de inte endast hälsar välkommen utan att användaren kan utföra något i e-tjänsterna. Senast då behöver den svenska strategin eller strategierna för att få tillgång till betrodd elektronisk behörighetsinformation från utlandet finnas på plats.

Först när behörighetsinformationen fungerar och e-tjänsterna är fullt inkopplade på ett tillförlitligt sätt, kan den fulla nyttan av eIDAS nås.

Inom ramen för genomförandet kommer mer detaljerade tidplaner och andra beslutsunderlag att tas fram.

9 Konsekvenser

EU-förordningar gäller som lag. Därmed måste Sverige införa de delar av förordningen som är obligatoriska. Inom e-legitimationsområdet omfattas dels delar av den svenska noden, dels offentliga organs erkännanden av utländska e-legitimationer.

9.1 Nyttor

Nyttorna som följd av ett lyckat eIDAS-införande kan uppstå inom åtminstone följande områden:

- Effektivisering och bättre offentlig service i svenska kommuners, landstings och statliga myndigheters ärendeflöden genom ökad digitalisering
- Svenska privatpersoner och företag får tillgång till digital service i offentlig och privat sektor utomlands
- Privat sektor i Sverige får dels möjligheter att elektroniskt identifiera kunder i sina digitala tjänster, dels möjligheter som leverantörer av e-legitimationer och betrodda tjänster

9.2 Konsekvenser för offentliga organ till följd av obligatoriet

De offentliga organ vars e-tjänster möjliggör inloggning med e-legitimation på minst tillitsnivå 3 måste som ett minimum göra följande:

- 1) kartlägga vilka e-tjänster som behöver anslutas till eIDAS
- 2) utöka listan över för användaren valbara inloggningssätt (anvisningstjänsten) och
- 3) svara med ett välkomstsmeddelande.

Kostnaden för detta förfarande är sannolikt låg, åtminstone för de myndigheter som anpassat sig till standarden SAML 2, och bör kunna utföras inom löpande förvaltning innan 28 september 2018, då obligatoriet börjar gälla. De som inte har gjort det kan t.ex. avropa hjälp på Kammarkollegiets ramavtal ”Programvaror och tjänster 2014”.

Myndigheter som aktivt väljer att släppa in individen i e-tjänsten efter förnyad riskanalys, har eventuellt anpassat e-tjänsterna på andra sätt. Nyttor och andra konsekvenser för detta får bedömas av respektive myndighet, t.ex. beträffande språkstöd och vilka personidentitetsbegrepp som ska användas.

9.3 Konsekvenser för svensk e-legitimationsförsörjning

Om svenska myndigheters riskanalys med anledning av eIDAS leder fram till att tillitsnivå hög (4) behövs i en eller flera e-tjänster, behövs det även svenska e-legitimationer som är kvalitetsmärkta på den högsta tillitsnivån. Då e-legitimationer på den högre tillitsnivån kan förväntas ha en mer begränsad spridning och användbarhet, kan konsekvenserna bli ett minskat nationellt användande av sådana e-tjänster. Det är därför viktigt att de svenska e-tjänsterna kan hantera den ökade riskexponering som följer av den gränsöverskridande e-legitimeringen med hjälp av kompenserande säkerhetskontroller, snarare än att dessa omständigheter driver krav på högre tillitsnivåer.

10 Sammanfattning av genomförda aktiviteter

Eva Sartorius, E-legitimationsnämnden, har varit utredningssekreterare. Arbetet har bedrivits med hjälp av:

- Arbetsmöten med myndigheter, experter och potentiella eID-leverantörer
- Avstämning av arbetshypoteser med bl.a. samrådsmyndigheterna i maj och augusti 2015
- Föredragningar av arbetshypoteser vid Näringsdepartementets små och stora referensgruppsmöten inom eIDAS
- Dialoger och föredrag vid Offentliga Rummet, Informationssäkerhetsdagarna, eFörvaltningsdagarna, Sundsvall 42 och Internetdagarna
- Skriftligt samråd under november - december 2015. Samrådssynpunkterna har arbetats in i den slutliga versionen av rapporten.

11 Bilaga – Behov av utländska e-legitimeringar

E-legitimationsnämnden genomförde under september 2015 en enkät riktad till svenska offentliga myndigheter. Bland svarsalternativen fanns det en valbar fritextmöjlighet att räkna upp exempel på administrativa flöden som rör utländska personer, dvs. där det skulle kunna vara aktuellt med utländska e-legitimationer om förutsättningarna skulle finnas på plats. Svaren omfattade (utan någon särskild ordning):

- Barnomsorg: ansökan, schema, inkomstanmälan, uppsägning
- Skolval, skolansökan, skolportal, skolskjuts, ansökan om fritidsplats, omdömen, frånvaro, lärplattform, kontakter med vårdnadshavare
- Bostadsförmedling
- Ansökan om försörjningsstöd
- Ansökan om äldreomsorg, andra insatser inom socialtjänsten
- Ansökan till skola/förskola
- Bibliotekslån
- Bygglov
- Uthyrning av stugor och lokaler
- Anlitande av utländska konsulter
- Mina vårdkontakter/1177.se, övrig vård och omsorg, t.ex. omsorgsdagboken
- Avlopp och sophantering
- Ekonomiskt bistånd
- Feriearbeten
- Guide och lots (via app) för nyanlända flyktingar, svenska för invandrare
- Parkeringstillstånd
- Utskänkningstillstånd
- Utländska fordonsägare som ska betala trängselskatt eller infrastrukturavgift.
- Utländska fordonsägare som ska betala parkeringsanmärkningar
- Personer med samordningsnummer som ska betala fordonsskatt
- Registrering av olyckor där iblandade saknar personnummer
- Ansökan om lokförarbevis, medicinsk dispens
- Tillfällig registrering av fordon, äga fordon
- Tillfällig ägare av fordon för export av fordon
- Inloggning för att rapportera egen kontroll och beställning av besiktning av fordon
- Jobbansökan
- Stipendier/forskningsanslag

- Alla företagsärenden utom där föreståndare behövs för enskild näringsidkare, föreståndaren behöver samordningsnummer i de fall personnummer saknas.
- Anmälan om kemiska produkter (Produktregistret)
- Ansöka om garanti för exportaffär
- Långvarig relation med pensionssparare och pensionärer
- Efterlevandepension
- Ansökan om registrering som fastighetsmäklare
- Ansökan om rättshjälp
- Ansökan till Försvarsmakten
- Auktorisation av tolkar och translatorer.
- Avverkningsanmälan
- Bidragsansökningar
- Delta i statistisk undersökning
- En ansökan om brottsskadeersättning från en person som inte är svensk medborgare
- Verksam.se: registrera företag (AB, Enskild firma m.m.), samt registrera F-skatt, moms och arbetsgivare
- Hundregistret
- Ansökan om importlicens
- Inom EU-gemensamma Tull- och skattesystemen finns det bedömt ett behov av utländska e-legitimationer. Likaså kan det finnas krav på att hantera personer utan personnummer.
- I flera av de måltyper som domstolarna hanterar
- Klagomål på vård och omsorg
- Kompletteringar av läkemedelsansökningar
- Kulturbidragsansökningar där norska samer deltar, flera kulturorganisationer har säte i Norge men rör samer i flera länder
- Legitimationsansökningar (t.ex. läkare)
- Min fastighet och Mina fastighetsärenden
- Patentansökan, varumärkesansökan, mönsterskyddsansökan, samt uppdrag inom dessa ärendetyper
- Rot/Rut-ärenden, ärenden inom punktskatteområdet, ärenden inom kontrolluppgiftshanteringen.
- Sjukpenning
- Antagning av internationella studenter
- Bekräfta utländska gästforskare
- Akademiska meriter/intyg

- Skapande av lokalt konto och återställning
- Universitetsstudenter från både Sverige, EU och tredje land. Det vore väldigt praktiskt att kunna använda andra länders e-legitimation men här kommer problemet med hur man gör kopplingen till den unika personen då man inte har något personnummer. Universiteten hanterar utländska personer i de studieadministrativa systemen inkl. antagningen, samt i personalsystemet. Dessa källsystem är därefter kopplade till andra system. Närliggande exempel är studieadministrativa system, studiemedel för studier i Sverige och utomlands, samt studiehjälp för studier i Sverige och utomlands
- Internatskolor
- Styrelsemedlemmar i stiftelser, jaktärenden, fastighetsfrågor, företag som ska etablera sig i Sverige
- Systemstöd för hantering av nyanlända. Gemensam jobbsökartjänst för de nordiska länderna.
- Såväl byggentreprenörer som järnvägsföretag och företag som söker tillstånd kopplade till vägtrafik kan vara utländska eller företrädas av personer utan svenskt personnummer. När det gäller byggarbetsplatser sker legitimering via det internationella identifieringssystemet ID06, eventuellt skulle en integrering av det systemet med e-legitimationer täcka delar av behovet.